

Service Center Recognition Image Processing System (SCRIPS) – Privacy Impact Assessment

PIA Approval Date – Feb. 13, 2007

System Overview

SCRIPS is a mission critical system utilizing high-speed scanning and digital imaging technology in processing tax documents. The SCRIPS system provides an integrated suite of hardware and software components that improves current Optical Character Recognition (OCR) tax form handling capabilities for the Internal Revenue Service (IRS). The SCRIPS is a stand alone, tax forms processing system. It replaced the OCR processing hardware and software applications, which previously processed single-side tax reporting forms (Federal Tax Deposits (FTD) and Information Returns Program (IRP) and Schedule K-1. SCRIPS applications have been developed for the processing of scanned tax forms - e.g., Federal Tax Deposits (FTD) and Information Returns Program (IRP- Forms 1096, 1098, 1099, and 5498). The IRS has now added certain K- documents to the scan list of form types.

Systems of Records Notice (SORN):

- IRS 22.034-Individual Returns Files, Adjustments and Miscellaneous Documents Files
- IRS 22.061-Individual Return Master File (IRMF) (formerly Wage and Information Returns Processing (IRP) File)
- IRS 24.030-Individual Master File (IMF), Taxpayer Services (formerly Individual Master File (IMF), Returns Processing)
- IRS 24.046-Business Master File (BMF), Taxpayer Services (formerly Business Master File (BMF), Returns Processing)
- IRS 34.037 for the audit trail records.

Data in the System

1. Describe the information (data elements and fields) available in the system in the following categories:

A. Taxpayer: Taxpayer data available in the system:

- Individual taxpayer name
- Business taxpayer name
- Individual taxpayer SSN
- Business EIN or other TIN
- Individual taxpayer address
- Business taxpayer address
- Assessed tax liability
- Payments
- Other credits
- Balance due amounts
- Refund checks sent
- Tax period
- Employment status
- Withholdings
- Wages earned
- Interest income
- Miscellaneous income
- Interest paid
- Dividends
- IRA contribution information

- Gambling winnings
- Proceeds from real estate transactions
- Proceeds from stock sales
- Tuition payments
- Student loan interest
- Name of Individual who holds Power of Attorney (POA)

B. Audit Trail Information: Is held in the system for the individual site System Security Officer (SSO) to review. A few auditable events are listed below:

- Logon/Logoff to system
- Change password
- Notations if a file has been opened
- Creation or Modification of user accounts
- All administrator actions

2. Describe/identify which data elements are obtained from files, databases, individuals, or any other sources.

A. IRS: The following IRS forms provide SCRIPS with all the data elements in the system:

- Form 940 Employer's Annual Federal Unemployment (FUTA) Tax Return
- Form 941 Employer's Quarterly Tax Return
- Form 1096, Annual Summary and Transmittal of U. S. Information Returns
- Form 1098, Mortgage Interest Statement
- Form 1098-E, Student Loan Interest Statement
- Form 1098-T, Tuition Payments Statement
- Form 1099-A, Acquisition, or Abandonment of Secured Property
- Form 1099-B, Proceeds From Broker and Barter Exchange Transactions
- Form 1099-C, Cancellation of Debt
- Form 1099-DIV, Dividends and Distribution
- Form 1099-G, Certain Government Payments
- Form 1099-H, Health Insurance Advance Payments
- Form 1099-INT, Interest Income
- Form 1099-MISC, Miscellaneous Income
- Form 1099-OID, Original Issue Discount
- Form 1099-PATR, Taxable Distributions Received From Cooperatives
- Form 1099-Q, Qualified Tuition Program Payments (Under Section 529)
- Form 1099-R, Distributions from Pensions, Annuities, Retirement or Profit-Sharing Plans, IRAs, Insurance Contracts, etc.
- Form 1099-S, Proceeds From Real Estate Transactions
- Form 5498, Individual Retirement Arrangement Information
- Schedule K-1 (Form 1065)
- Schedule K-1 (Form 1041)
- Schedule K-1 (Form 1120S)
- Form 8109, Federal Tax Deposit (FTD) (pre-printed) Coupon 327, 328
- Form 8109B, Federal Tax Deposit (FTD) (handwritten) Coupon 327, 328

- B. Taxpayer – The individual Taxpayer can choose to submit anyone of the previously mentioned forms.
- C. Other Federal Agencies: Federal agencies as employers may potentially submit any of the stated Form types as it relates to tax administration. The only paper processing allowed by IRS is for small monetary amounts.
- D. State and Local Agencies: Over a certain monetary threshold State and Local agencies must file electronically, therefore, it is inconceivable that any State or local agencies would provide any of the previous mentioned paper forms as paper submission.
- E. Other third party sources: Bank and financial institutions, over a certain monetary threshold, must file electronically; therefore making it impossible that any of these third parties would provide any of the previous mentioned paper forms as paper submission.

3. Is each data item required for the business purpose of the system? Explain.

Yes. The individual taxpayer can choose to submit any one of the previously mentioned forms in paper format.

4. How will each data item be verified for accuracy, timeliness, and completeness?

All SCRIPS data are received from authoritative sources e.g., taxpayer, employer, shareholder, etc., through the mail in paper format.

As the data are retrieved for each of the fields, it is checked for completeness and validity. The SCRIPS application requires the user to manually enter data for any field that cannot be deciphered, or does not meet length and appropriate character requirements by the character recognition engine. If none of the form can be deciphered, the user must enter the form manually. Any field entered by the user, is again checked against length and appropriate character requirements by the application. If the entered data does not meet requirements, the application will display an error message explaining the requirement to be met, and data must be re-entered.

FTDs must be processed within a 24-hour period; K-1 and IRP forms must be processed by their IRM and location Production Completion Date (PCD).

5. Is there another source for the data? Explain how that source is or is not used.

Bank and financial institutions over a certain monetary threshold must file electronically; therefore, it is impossible that any of these third parties would provide any of the previous mentioned paper forms as paper submission.

6. Generally, how will data be retrieved by the user?

Each SCRIPS workstation presents an authorized user with several “main menu” options, which in turn have several sub-menus or modules attached to them. Some of these submenus provide the user with the option to query or run reports on SCRIPS data.

The submenus are listed below:

- Document Review
- Profile Maintenance
- Workflow Maintenance
- Workflow Status
- DLN/SN Maintenance
- Output Selection
- Server Access TE

- Reports
- Number of blocks
- System reporting
- Vendor Code Maintenance

7. Is the data retrievable by a personal identifier such as name, SSN, or other unique identifier?

To bring up a file the user must enter a Document Locator Number (DLN). Every form that is scanned has a DLN that is generated specifically for that document.

Access to the Data

8. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Others)?

A profile is first established for each authorized user by the SCRIPS System Administrator through OL 5081. The user is then authorized by the SCRIPS Site Manager. Permissions are grouped by SCRIPS Users, SCRIPS Managers, SCRIPS Contractor-Developers, Others (e.g., TIGTA and GAO users), which lists only those functions that the user is authorized to execute. Currently, the following roles for SCRIPS exist: transport operators; system administrators; supervisors; quality reviewers; and workstations operators.

Below is a description of the permissions associated with each user:

Role: Transport Operators

Permissions: Powering up and down equipment, log on/off monitors, execute runs on scanner, handle system errors and problems, image degradation.

Role: System Administrators

Permissions: Maintain/manage: user accounts, audit trail files, security measures, backup files, network, database, system recovery, and restore backup.

Role: Supervisory Personnel

Permissions: Sets operator files, manage operator workflow, run reports, manage recovery, purge files, manage tape output and input, update tables, respond to error messages, and handle system priorities and parameters.

The SCRIPS application was contracted to and developed by Northrop Grumman Information Technology, Inc who will have continued access to SCRIPS for maintenance and trouble shooting issues.

9. How is access to the data by a user determined and by whom?

The SCRIPS site manager authorizes access to the system via the access control process (OL 5081). Users must complete and submit access forms using OL 5081 to their manager for approval. Then the System Administrator sets the permissions.

Application users are given only access rights necessary to complete the tasks associated with their job description. The application separates user function by role.

Northrop Grumman contractors have minimum background investigation (MBI) and undergo the same security training as IRS employees.

10. Do other IRS systems provide, receive, or share data in the system? If YES, list the system(s) and describe which data are shared.

Yes. Beginning with the Tax Year 2003 processing year, SCRIPS will use Files Transfer Protocol (FTP) via the Enterprise FTP Network Server (EFNS), to transmit data to IRS Computing Centers (MCC or TCC).

11. Have the IRS systems described in Item 10 received an approved Security Certification and Privacy Impact Assessment?

Enterprise FTP Network Server (EFNS)

- Privacy Impact Assessment (PIA) – 4/19/2002, expired 4/19/2005
- Certification & Accreditation information not available.

12. Will other agencies provide, receive, or share data in any form with this system?

The SCRIPS application provides information with TIGTA and GAO. This only takes place during audits.

Administrative Controls of Data

13. What are the procedures for eliminating the data at the end of the retention period?

Destruction of the secured media for stored SCRIPS' data will be or are in the IS data security mandates. Since SCRIPS data are optical, and the IRS has not yet set standards for destruction of any optical media, physical destruction of the optical media shall be by shattering into shards less than ½" in size [until further guidance is supplied].

Data retention periods are as follows: IRM cite -- Records Control Schedule for Submissions Processing Campus Records 07-01-2005

- All IRP Forms as previously listed = 4 years [IRM Exhibit 1.15.29-3 56, 98, 85, 87, 88, 122, 129, 222, 342, 343]
- Schedule K-1 U.S. Partnership Return of Income (Form 1065) = 7 years - IRM 1.15.29-3 part 56
- Schedule K-1 U.S. Fiduciary Income Tax Return (For Estate and Trusts) (Form 1041) = 7 years - IRM 1.15.29-3 part 56
- Schedule K-1 U.S. Small Business Corporation Return of Income (Form 1120S) = 75 years - IRM 1.15.29-3 part 58
- Federal Tax Deposit (FTD) (preprinted) Coupon (Form 8109, and Form 8109B)= 7 years - IRM 1.15.29-3 parts 65, 342,343]
- Form 940 Employer's Annual Federal Unemployment (FUTA) Tax Return = 7 years - IRM 1.15.29-3 part 65
- Form 941 Employer's Quarterly Tax Return = IRM 1.15.29-3 part 65

All audit trail files for IRS systems are retained for a minimum period of six years SCRIPS keeps them for 12 years. Electronic records are protected in accordance with the sensitivity of the information stored.

For systems that store or process taxpayer information, audit trail archival logs are retained for six (6) years, unless otherwise specified by a formal Records Retention Schedule developed in accordance with IRM 1.15, Records Management.

The IRS retains audit log data, along with other system-specific records, as specified by a system records retention schedule for the system in question. See IRM 1.15, *Records Management*, for specific guidance regarding system records retention schedules. Audit logs may be retained up to seven (7) years, per IRM 1.15. IRM 1.15 has precedence over this IRM for systems covered by IRM 1.15.

14. Will this system use technology in a new way?

No.

15. Will this system be used to identify or locate individuals or groups? If so, describe the business purpose for this capability.

No. The system as designed does not have the capability to monitor individuals except as it pertains to the audit trail information which is used to identify unauthorized events.

16. Will this system provide the capability to monitor individuals or groups? If yes, describe the business purpose for this capability and the controls established to prevent unauthorized monitoring.

No. The system as designed does not have the capability to identify, locate or monitor groups.

17. Can use of the system allow IRS to treat taxpayers, employees, or others, differently?

No. There is no possibility for disparate treatment with the SCRIPS because SCRIPS only makes an image and processes the Forms as they are received from the mailroom.

18. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?

Not Applicable.

19. If the system is web-based, does it use persistent cookies or other tracking devices to identify web visitors?

Not Applicable. SCRIPS is a stand alone, tax forms processing nonweb-based system and its operation does not require the use persistent cookies or other tracking devices for identification.

[View other PIAs on IRS.gov](#)

Next Steps

Once completed, submit the PIA to the Office of Privacy. A Privacy Analyst will review and conduct an analysis of the submitted PIA. Once the Office of Privacy determines that the system's privacy compliance is adequate, the Office of Privacy will issue an approval memo for the system. The approval memo will identify any residual privacy risks. The approval memo should be retrained in the system records. The system must be reviewed again in three years, or if the system undergoes a major change.